



Fraud Focus: Protecting What Matters

Summer 2026

PHONE SCAMS ARE ON THE RISE

Phone scams continue to increase across the country, with fraudsters using sophisticated tactics to impersonate trusted organizations, financial institutions, government agencies, and even local businesses. The rapid advancement of artificial intelligence (AI) has made these scams even more convincing. Criminals can now use AI to create realistic voice clones, generate convincing messages, and automate scam campaigns at a scale that was not previously possible. In some cases, scammers may even use AI-generated audio to mimic the voice of a family member, coworker, or trusted representative.

These scammers often create a sense of urgency or fear, hoping to pressure individuals into acting before they have time to verify the situation.

Common scam tactics include callers claiming there is an alert on your account that requires immediate attention, a suspicious payment or transaction that needs to be verified, or other urgent account-related issues. Their goal is to create concern and pressure you into providing information, account details, passwords, or payment through unusual methods such as wire transfers, gift cards, or cryptocurrency.

Scammers can also use caller ID spoofing technology to make it appear as though they are calling from a legitimate organization. Combined with AI-generated voices and messages, these tactics can make fraudulent communications appear increasingly authentic.

What should you do?

- Pause and verify before taking any action
- Hang up and contact Northwest Bank using a trusted phone number from our website, account statement, or other verified source
- Never share passwords, one-time passcodes, verification codes, or MFA authentication codes
- Do not click links or open attachments sent through unsolicited calls, text messages, or emails
- Review your account activity regularly and report anything suspicious immediately
- Trust your instincts—if something feels unusual, urgent, threatening, or too good to be true, it may be a scam

Northwest Bank will never ask you for your password or MFA. If something simply doesn't feel right, hang up and contact your local Northwest Bank customer service team using a trusted phone number.

We can help you verify requests and take steps to protect your accounts.

Tools to Help Protect Your Accounts

Multi-Factor Authentication (MFA)

Multi-Factor Authentication **adds an extra layer of security to your online banking experience** by requiring additional verification beyond just a password. Contact your local customer service team for information on how to register.

Benefits of MFA include:

- Enhanced protection against unauthorized access
- Reduced risk of compromised passwords
- Increased account security for online and mobile banking

Account Monitoring

One of the most effective ways to detect fraud early is to actively monitor your accounts and transaction activity by regularly:

- Review account balances and transaction history
- Verify checks, ACH transactions, and debit card purchases
- Monitor online banking login activity
- Report unauthorized or suspicious activity immediately

Account Alerts

Timely notifications can serve as an early warning system, helping you detect suspicious activity, unauthorized transactions, or potential fraud.

- Login notifications
- Debit card transactions
- Low balance warnings
- Large withdrawals or transfers
- ACH and wire activity

Services We Offer to Help Protect Your Accounts

Check Positive Pay

Check Positive Pay is a fraud prevention service designed to help business clients detect and prevent check fraud.

The service helps protect against counterfeit, altered, duplicate, and unauthorized checks by identifying exceptions for review before payment is processed, giving businesses greater control over check disbursements and reducing exposure to fraud.

ACH Filters

ACH Filters can help businesses proactively monitor and control electronic transactions posting to their accounts by identifying and blocking unauthorized ACH activity.

This powerful fraud prevention tool enables businesses to establish approved transaction criteria and receive greater visibility into account activity, helping safeguard company funds.